INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/21847

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00; G06F 11/30,12/14,9/32; H04M 15/00; H04N 7/167; H04K 1/04,1/06
US CL : 713/171,193,194; 380/203,210,259,273,37,281; 379/120
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/171,193,194; 380/203,210,259,273,37,281; 379/120

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	X US 2001/0029581 (KNAUFT) 11 October 2001 (11.11.2001), ¶48, ¶75-86, Fig. 5A, #514, Fig. 5B, #522	1-39
X,P	US 6,690,795 B1 (RICHARDS) 10 February 2004, columns 5-10.	
---		---
Y,P		1-39
X	US Re. 33,189 (LEE et al) 27 March 1990 (27.03.1990), column 2, line 37 - column 4, line 36.	
---		---
Y		1-39
Y	MENEZES et al. Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, BOCA Raton, FL, CRC Press, US, 1997, pp. 551-553, 557-581.	1-39

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2004 (18.11.2004)	23 DEC 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Greg Morse Peggy Harrod Telephone No. (571) 272-3838

Form PCT/ISA/210 (second sheet) (January 2004)

REC'D 29 DEC 2004
WIPO PCT

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
MILAN PATEL
5775 MOREHOUSE DRIVE
SAN DIEGO, CA 92121-1714

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*) 23 DEC 2004

Applicant's or agent's file reference
030441WO

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US04/21847	08 July 2004 (08.07.2004)	08 July 2003 (08.07.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): H04L 9/00; G06F 11/30,12/14,9/32; H04M 15/00; H04N 7/167; H04K 1/04,1/06 and US Cl.: 713/171,193,194; 380/203,210,259,273,37,281; 379/120

Applicant

HAWKES ET AL.

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [x] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Greg Morse Peggy Harrod
Telephone No. (571) 272-3838

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/21847

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ in written format

☐ in computer readable form

c. time of filing/furnishing

☐ contained in international application as filed.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/21847

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-39	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-39	NO
Industrial applicability (IA)	Claims	NONE	YES
	Claims	NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/21847

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

Regarding claims 5, 13, 19, 25, 31 & 37, "the secret key" does not appear in the claim or any of it's depending claims. The references to "the secret key" are understood to mean "the access key" in these claims.

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1-39 lack inventive step over U.S. Patent Re. 33,189 to Lee et al. (Lee) in view of Handbook of Applied Cryptography by Menezes et al. (Menezes).

Regarding claims 1, 16 & 28, Lee discloses distributing a key/user ID (col. 3, lines 28-42), receiving a secret key encrypted by the key/user ID (col. 4, lines 1-22), decrypting the secret key/ key by the key/user ID (col. 4, lines 1-22), receiving the access key/random number encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random number by the secret key/key (col. 4, lines 1-22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 2, 8, 11, 15, 17, 21, 23, 27, 29, 33, 35 & 39, Lee discloses the secret key being a temporary key/key of the month (col. 3, lines 28-42).

Regarding claims 3 & 9, Lee discloses deriving a short key/PN sequence based on the access key/random number, receiving encrypted broadcast content/video and decrypting the encrypted broadcast content using the short key/PN sequence (col. 3, line 28 - col. 4, line 22).

Regarding claims 4, 18 & 30, Lee discloses distributing a key/user ID (col. 3, lines 28-42), receiving the access key/key encrypted by the key/user ID and decrypting the access key/key by the private key/user ID (col. 4, lines 1-22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 5, 13, 19, 25, 31 & 37, as best understood, Lee discloses the access key being a temporary key (key of the month) (col. 3, lines 28-42).

Regarding claim 6, Lee discloses deriving a short key/random number based on the access key/key, receiving encrypted broadcast content/video and decrypting the encrypted broadcast content/video using the short key/random number (col. 3, line 28 - col. 4, line 22).

Regarding claims 7, 20 & 32, Lee discloses receiving a key/user ID corresponding to a private key/user ID (col. 3, lines 28-42), encrypting the secret key/key with the key/user ID (col. 3, lines 42-64), sending the encrypted secret key/key (col. 3, lines 1-22), receiving the access key/random number encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random number by the secret key/key (col. 3, line 28 - col. 4, line 22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 10, 22 & 34, Lee discloses receiving a key/user ID (col. 3, lines 28-42), encrypting a secret key/key using the key/user ID (col. 3, lines 42-64), sending the encrypted secret key/key (col. 4, lines 1-5), encrypting the access key/random number using the secret key/key (col. 3, lines 42-64) and sending the encrypted access key/random number (col. 4, lines 1-22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 12, 24 & 36, Lee discloses receiving a key/user ID (col. 4, lines 1-22), encrypting the access key/key using the key/user ID (col. 3, lines 42-64) and sending the encrypted access key/key (col. 3, lines 42-64). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 14, 26 & 38, Lee discloses distributing a key/user ID corresponding to a private key/user ID (col. 3, lines 28-42), receiving a secret key/key (col. 3, lines 42-64) encrypted by the key/user ID (col. 3, lines 42-64), decrypting the secret key/key by the private key/user ID (col. 4, lines 1-22), encrypting the access key/random number by the secret key/key (col. 3, lines 42-64) and sending the encrypted access key/random number (col. 3, line 28 - col. 4, line 22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

US Re. 33,189 (LEE et al) 27 March 1990 (27.03.1990), column 2, line 37 - column 4, line 36.

MENEZES et al. Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, BOCA Raton, FL, CRC Press, US, 1997, pp. 551-553, 557-581.